PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-101459
(43)Date of publication of application : 05.04.2002

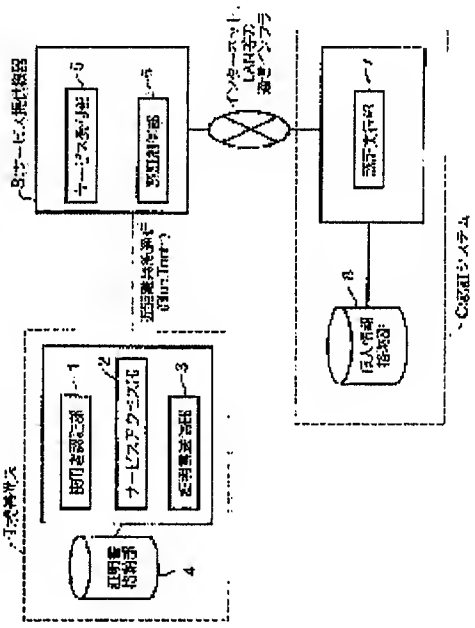
(51)Int.Cl. H04Q 7/38
G06F 15/00
G09C 1/00
H04L 9/32

(21)Application number : 2000-291119
(22)Date of filing : 25.09.2000

(71)Applicant : NTT COMWARE CORP
(72)Inventor : OZURU NOBUHIKO
KITAOKA KATSUYA
OMURO HISAKO
NAGAOKA TORU
KOBAYASHI KAZUE

(54) PORTABLE TERMINAL AND SERVICE PROVIDING DEVICE HAVING PERSON IN QUESTION AUTHENTICATION FUNCTION, AND ITS SYSTEM AND PROCESSING METHOD CONSISTING OF ITS PROCESSING PROCEDURES, AND ITS RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a portable terminal and a service providing device that can simply authenticate a person in question in a service providing environment needing authentication of the person in question, receive the provision of a desired service, and to provide its system and a processing method consisting of its processing procedures and its recording medium.
SOLUTION: The portable terminal of this invention is connected to the service providing device through radio communication that stores an electronic certificate used for authenticating a person in question, authenticates the person in question and provides a service to a legal user, the service providing device of this invention transmits a connection application program used to select a provided service on the portable terminal to the portable terminal, the portable terminal executes the connection application program, transmits the electronic certificate to the service providing device, and the service providing device authenticates the person in question based on the received electronic certificate so as to decide the propriety of starting the service provision.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号
特開2002－101459
（P2002－101459A）
(43)公開日　平成14年４月５日(2002.4.5)

(51)Int.Cl.⁷	識別記号	FI		テーマコード（参考）
H04Q 7/38		G06F 15/00	330A	5B085
G06F 15/00	330	G09C 1/00	640Z	5J104
G09C 1/00	640	H04B 7/26	109R	5K067
H04L 9/32		H04L 9/00	675A	
			675D	

審査請求　有　　請求項の数12　ＯＬ　（全 12 頁）

(21)出願番号　特願2000－291119(P2000－291119)

(22)出願日　平成12年９月25日(2000.9.25)

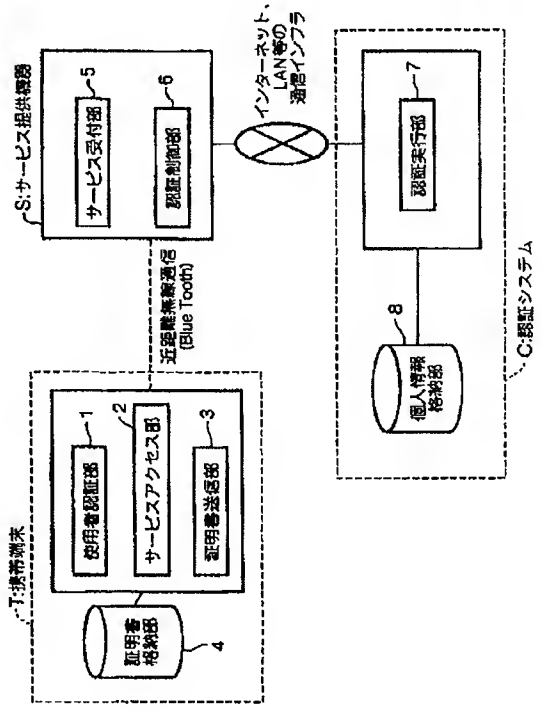
特許法第64条第２項ただし書の規定により図面第７図，８図の一部は不掲載とした。

(71)出願人　397065480
エヌ・ティ・ティ・コムウェア株式会社
東京都港区港南一丁目９番１号
(72)発明者　大鶴　暢彦
東京都港区港南一丁目９番１号　エヌ・ティ・ティ・コミュニケーションウェア株式会社内
(72)発明者　北岡　勝也
東京都港区港南一丁目９番１号　エヌ・ティ・ティ・コミュニケーションウェア株式会社内
(74)代理人　100064908
弁理士　志賀　正武　（外２名）

最終頁に続く

(54)【発明の名称】　本人認証機能を有する携帯端末及びサービス提供機器、ならびに、そのシステム及びその処理手順からなる処理方法及びその記録媒体

(57)【要約】
【課題】　本人認証を必要とするサービス提供環境において、簡易に本人認証を行え、所望のサービスの提供を享受できる本人認証機能を有する携帯端末及びサービス提供機器、ならびに、そのシステム及びその処理手順からなる処理方法及びその記録媒体を提供する。
【解決手段】　本発明による携帯端末は、本人認証のために用いる電子証明書を記憶し、本人認証を行い正当なユーザにサービスを提供するサービス提供機器と無線通信により接続され、本発明によるサービス提供機器は、提供するサービスを携帯端末上で選択可能とする接続アプリケーションプログラムを携帯端末に送信し、携帯端末はこの接続アプリケーションプログラムを実行して電子証明書をサービス提供機器に送信し、サービス提供機器は、受信した電子証明書に基づき本人認証を行いサービス提供開始の可否を決定する。



【特許請求の範囲】
【請求項１】　本人認証を行い正当なユーザにサービスを提供するサービス提供機器と無線通信により接続され、該サービス提供機器からサービスの提供を受けるために使用可能な携帯端末であって、
該携帯端末は、
前記サービス提供機器において本人認証のために用いる電子証明書を記憶する記憶部を備え、前記サービス提供機器からの要求に応じて、該電子証明書を前記サービス提供機器に送信することを特徴とする本人認証機能を有する携帯端末。
【請求項２】　本人認証を行い正当なユーザにサービスを提供するサービス提供機器と通信により接続され、該サービス提供機器からサービスの提供を受けるために使用可能な携帯端末であって、
該携帯端末を現に使用するユーザが正当なユーザであることを該携帯端末において識別するために登録された個人識別情報と、前記サービス提供機器において本人認証のために用いる電子証明書を記憶する記憶部と、
前記個人識別情報を入力するための入力部と、
前記入力部に入力された個人識別情報と前記登録された個人識別情報とを照合し、前記個人識別情報を入力したユーザが正当なユーザであるか否かを判定する使用者認証部と、
前記使用者認証部の判定により、前記個人識別情報を入力したユーザが正当なユーザであると判定された場合、該ユーザによる所定の操作により、前記サービス提供機器に向け接続要求を送り、該接続要求により前記サービス提供機器と該携帯端末間で接続が確立後、該サービス提供機器から送られ該サービス提供機器が提供するサービスを選択可能とする接続アプリケーションプログラムを受信するとともに実行するサービスアクセス部と、
前記サービス提供機器から送信される電子証明書送信要求を受けた場合、前記記憶部に記憶された電子証明書を該サービス提供機器に送信する証明書送信部と、を具備することを特徴とする本人認証機能を有する携帯端末。
【請求項３】　前記記憶部は、
前記携帯端末に対し着脱可能なメモリカードからなり、前記個人識別情報と電子証明書を記憶した該メモリカードを、前記携帯端末と独立して可搬可能としたことを特徴とする請求項１または請求項２に記載の本人認証機能を有する携帯端末。
【請求項４】　前記サービスアクセス部は、さらに、
前記サービス提供機器が複数あり、前記接続要求に対し複数のサービス提供機器が応答し該複数のサービス提供機器と接続可能な場合、該複数のサービス提供機器を任意に選択可能とすることを特徴とする請求項２ないし請求項３のいずれかに記載の本人認証機能を有する携帯端末。
【請求項５】　本人認証を行い正当なユーザにサービスを提供するサービス提供機器であって、
ユーザに対し、該ユーザが使用する携帯端末上で該サービス提供機器が提供するサービスを選択可能とする接続アプリケーションプログラムを記憶する記憶部と、
前記携帯端末から無線通信により送信される接続要求を受け接続を確立し、該携帯端末に対し、前記記憶部に記憶された接続アプリケーションプログラムを前記携帯端末へ送信し、該携帯端末から該サービス提供機器が提供するサービスを要求するサービス要求を受けるサービス受付部と、
前記サービス受付部が前記携帯端末からサービス要求を受けると、該携帯端末へ、該携帯端末を使用するユーザの電子証明書を要求する電子証明書要求を送信し、該携帯端末から電子証明書を受け、該電子証明書に基づき本人認証を行い、前記ユーザが正当なユーザであると判定された場合、前記サービス要求に応じたサービスの提供を開始させる認証制御部と、を具備することを特徴とする本人認証機能を有するサービス提供機器。
【請求項６】　前記認証制御部は、
本人認証のために用いる電子証明書を発行し本人認証を行う認証機関の認証システムに通信回線を介して接続され、
前記携帯端末から送信された電子証明書を前記認証機関の認証システムに転送し、該認証システムから前記ユーザが正当なユーザであるか否かの判定結果からなる情報を受け、前記本人認証を行うことを特徴とする請求項５に記載の本人認証機能を有するサービス提供機器。
【請求項７】　本人認証を行い正当なユーザにサービスを提供する請求項５に記載のサービス提供機器と、該サービス提供機器と無線通信により接続され、該サービス提供機器からサービスの提供を受けるために使用する無線通信可能な請求項１に記載の携帯端末と、から構成されることを特徴とする本人認証機能を有する携帯端末及びサービス提供機器からなるシステム。
【請求項８】　本人認証を行い正当なユーザにサービスを提供するサービス提供機器と無線通信により接続され、該サービス提供機器からサービスの提供を受けるために使用する無線通信可能な携帯端末における処理方法であって、
前記個人識別情報の入力を受ける手順と、
前記携帯端末を現に使用するユーザが正当なユーザであることを該携帯端末において識別するために予め登録された個人識別情報と前記入力された個人識別情報とを照合し、前記個人識別情報を入力したユーザが正当なユーザであるか否かを判定する手順と、
前記判定により、前記個人識別情報を入力したユーザが正当なユーザであると判定された場合、該ユーザによる所定の操作により、前記サービス提供機器に向け接続要求を送る手順と、
前記接続要求により前記サービス提供機器と該携帯端末

間で接続が確立後、該サービス提供機器から送られ該サービス提供機器が提供するサービスを受けるために使用される接続アプリケーションプログラムを受信し実行する手順と、
前記接続アプリケーションプログラムによる操作環境において、前記ユーザによる指定に応じたサービス要求を前記サービス提供機器へ送る手順と、
前記サービス要求に応じて前記サービス提供機器から送られる電子証明書送信要求を受け、予め記憶された電子証明書を該サービス提供機器に送信する手順と、を含むことを特徴とする本人認証機能を有する携帯端末における処理方法。
【請求項９】　本人認証を行い正当なユーザにサービスを提供するサービス提供機器における処理方法であって、
前記携帯端末から無線通信により送信される接続要求を受け接続を確立する手順と、
前記接続要求により該サービス提供機器と前記携帯端末間で接続が確立後、該サービス提供機器が提供するサービスを前記ユーザが受けるために使用される接続アプリケーションプログラムを前記携帯端末へ送信する手順と、
前記携帯端末上で実行された前記接続アプリケーションプログラムによる操作環境において前記ユーザによる指定に応じて送られるサービス要求を受ける手順と、
前記サービス要求に応じて、前記携帯端末に対し電子証明書を要求する電子証明書要求を送信する手順と、
前記携帯端末から送信される電子証明書を受け、該電子証明書に基づき本人認証を行う手順と、
前記本人認証で前記ユーザが正当なユーザであると判定された場合、前記サービス要求に応じたサービスを提供する手順と、を含むことを特徴とする本人認証機能を有するサービス提供機器における処理方法。
【請求項１０】　前記処理方法は、さらに、
前記携帯端末から送信された電子証明書を、該電子証明書を発行し本人認証を行う認証機関の認証システムに転送する手順と、
該認証システムから前記ユーザが正当なユーザであるか否かの判定結果からなる情報を受け、前記本人認証を行う手順と、を含むことを特徴とする請求項９に記載の本人認証機能を有するサービス提供機器における処理方法。
【請求項１１】　コンピュータ装置にインストールすることにより、その装置が請求項８に記載の方法を実行する装置となるソフトウェアが記録されたコンピュータ読取可能な記録媒体。
【請求項１２】　コンピュータ装置にインストールすることにより、その装置が請求項９または請求項１０に記載の方法を実行する装置となるソフトウェアが記録されたコンピュータ読取可能な記録媒体。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、本人性を保証する電子証明書を記憶させた携帯端末と、認証を伴うサービスを提供する各種サービス提供機器とを、通信により接続し、機器毎の認証を伴うサービスの提供ならびにその享受を実現する装置及び方法に関する。
【０００２】
【従来の技術】従来より実施されている本人を認証する方法として、例えば、免許証、パスポートなどの写真つき証明書の提示や、特別な装置を用いた指紋認証、眼球認証等がある。また、インターネット上で行われる本人認証では、例えば、認証機関から発行された電子証明書をパーソナルコンピュータ上のブラウザ等にインポートし、インターネットを介して相手に提示することによって本人認証を行っている。また、利用の際に認証を必要とする設備・機器では、磁気カード、ＩＣカード等を用いて、これらの設備・機器に設置されたカードリーダから利用者の登録情報を読み込ませたり、あるいは、利用者自身が、登録されたパスワード等の入力を行い本人認証を行っている。
【０００３】
【発明が解決しようとする課題】従来の免許証やパスポートなどの写真つき証明書の提示による方法では、人手を介した本人認証しか実現できない。また、特別な装置による指紋認証や眼球認証方式の場合、その装置を利用できる環境（施設）内のみでしか使用できず、一般的・汎用的な（場所が固定されない）サービス提供環境における本人認証の実現は困難である。また、インターネット上で、認証機関から発行された電子証明書をパーソナルコンピュータ上のブラウザ等にインポートする方式の場合、そのパーソナルコンピュータ上のみでしか電子証明書を使用できず、また利用対象もインターネット上のサイトに限定されている。また、利用の際に認証を必要とする設備・機器において、これらの設備・機器に設置されたカードリーダから利用者のカードに記録された登録情報を読み込ませたり、あるいは、利用者自身が、登録されたパスワード等の入力を行い本人認証を行う場合、こうした手段は、認証のみ行え、これらの設備・機器から提供される多様なサービスに容易に対応できるものではなく、また、利便性も低い。
【０００４】本発明は、上記の点に鑑みてなされたもので、本人認証を必要とするサービス提供環境において、簡易に本人認証を行え、所望のサービスの提供を享受できる本人認証機能を有する携帯端末及びサービス提供機器、ならびに、そのシステム及びその処理手順からなる処理方法及びその記録媒体を提供するものである。
【０００５】
【課題を解決するための手段】本発明の本人認証機能を有する携帯端末は、本人認証を行い正当なユーザにサー

ビスを提供するサービス提供機器と無線通信により接続され、該サービス提供機器からサービスの提供を受けるために使用可能な携帯端末であって、該携帯端末は、前記サービス提供機器において本人認証のために用いる電子証明書を記憶する記憶部を備え、前記サービス提供機器からの要求に応じて、該電子証明書を前記サービス提供機器に送信することを特徴とする。

【０００６】また、本発明の本人認証機能を有する携帯端末は、本人認証を行い正当なユーザにサービスを提供するサービス提供機器と通信により接続され、該サービス提供機器からサービスの提供を受けるために使用可能な携帯端末であって、該携帯端末を現に使用するユーザが正当なユーザであることを該携帯端末において識別するために登録された個人識別情報と、前記サービス提供機器において本人認証のために用いる電子証明書を記憶する記憶部と、前記個人識別情報を入力するための入力部と、前記入力部に入力された個人識別情報と前記登録された個人識別情報とを照合し、前記個人識別情報を入力したユーザが正当なユーザであるか否かを判定する使用者認証部と、前記使用者認証部の判定により、前記個人識別情報を入力したユーザが正当なユーザであると判定された場合、該ユーザによる所定の操作により、前記サービス提供機器に向け接続要求を送り、該接続要求により前記サービス提供機器と該携帯端末間で接続が確立後、該サービス提供機器から送られ該サービス提供機器が提供するサービスを選択可能とする接続アプリケーションプログラムを受信するとともに実行するサービスアクセス部と、前記サービス提供機器から送信される電子証明書送信要求を受けた場合、前記記憶部に記憶された電子証明書を該サービス提供機器に送信する証明書送信部と、を具備することを特徴とする。

【０００７】また、本発明の本人認証機能を有する携帯端末において、前記記憶部は、前記携帯端末に対し着脱可能なメモリカードからなり、前記個人識別情報と電子証明書を記憶した該メモリカードを、前記携帯端末と独立して可搬可能としたことを特徴とする。

【０００８】また、本発明の本人認証機能を有する携帯端末において、前記サービスアクセス部は、さらに、前記サービス提供機器が複数あり、前記接続要求に対し複数のサービス提供機器が応答し該複数のサービス提供機器と接続可能な場合、該複数のサービス提供機器を任意に選択可能とすることを特徴とする。

【０００９】また、本人認証機能を有するサービス提供機器は、本人認証を行い正当なユーザにサービスを提供するサービス提供機器であって、ユーザに対し、該ユーザが使用する携帯端末上で該サービス提供機器が提供するサービスを選択可能とする接続アプリケーションプログラムを記憶する記憶部と、前記携帯端末から無線通信により送信される接続要求を受け接続を確立し、該携帯端末に対し、前記記憶部に記憶された接続アプリケーションプログラムを前記携帯端末へ送信し、該携帯端末から該サービス提供機器が提供するサービスを要求するサービス要求を受けるサービス受付部と、前記サービス受付部が前記携帯端末からサービス要求を受けると、該携帯端末へ、該携帯端末を使用するユーザの電子証明書を要求する電子証明書要求を送信し、該携帯端末から電子証明書を受け、該電子証明書に基づき本人認証を行い、前記ユーザが正当なユーザであると判定された場合、前記サービス要求に応じたサービスの提供を開始させる認証制御部と、を具備することを特徴とする。

【００１０】また、本発明の本人認証機能を有するサービス提供機器において、前記認証制御部は、本人認証のために用いる電子証明書を発行し本人認証を行う認証機関の認証システムに通信回線を介して接続され、前記携帯端末から送信された電子証明書を前記認証機関の認証システムに転送し、該認証システムから前記ユーザが正当なユーザであるか否かの判定結果からなる情報を受け、前記本人認証を行うことを特徴とする。

【００１１】また、本発明の本人認証機能を有する携帯端末及びサービス提供機器からなるシステムは、本人認証を行い正当なユーザにサービスを提供する請求項５に記載のサービス提供機器と、該サービス提供機器と無線通信により接続され、該サービス提供機器からサービスの提供を受けるために使用する無線通信可能な請求項１に記載の携帯端末と、から構成されることを特徴とする。

【００１２】また、本発明の本人認証機能を有する携帯端末における処理方法は、本人認証を行い正当なユーザにサービスを提供するサービス提供機器と無線通信により接続され、該サービス提供機器からサービスの提供を受けるために使用する無線通信可能な携帯端末における処理方法であって、前記個人識別情報の入力を受ける手順と、前記携帯端末を現に使用するユーザが正当なユーザであることを該携帯端末において識別するために予め登録された個人識別情報と前記入力された個人識別情報とを照合し、前記個人識別情報を入力したユーザが正当なユーザであるか否かを判定する手順と、前記判定により、前記個人識別情報を入力したユーザが正当なユーザであると判定された場合、該ユーザによる所定の操作により、前記サービス提供機器に向け接続要求を送る手順と、前記接続要求により前記サービス提供機器と該携帯端末間で接続が確立後、該サービス提供機器から送られ該サービス提供機器が提供するサービスを受けるために使用される接続アプリケーションプログラムを受信し実行する手順と、前記接続アプリケーションプログラムによる操作環境において、前記ユーザによる指定に応じたサービス要求を前記サービス提供機器へ送る手順と、前記サービス要求に応じて前記サービス提供機器から送られる電子証明書送信要求を受け、予め記憶された電子証明書を該サービス提供機器に送信する手順と、を含むこ

とを特徴とする。

【００１３】また、本発明の本人認証機能を有するサービス提供機器における処理方法は、本人認証を行い正当なユーザにサービスを提供するサービス提供機器における処理方法であって、前記携帯端末から無線通信により送信される接続要求を受け接続を確立する手順と、前記接続要求により該サービス提供機器と前記携帯端末間で接続が確立後、該サービス提供機器が提供するサービスを前記ユーザが受けるために使用される接続アプリケーションプログラムを前記携帯端末へ送信する手順と、前記携帯端末上で実行された前記接続アプリケーションプログラムによる操作環境において前記ユーザによる指定に応じて送られるサービス要求を受ける手順と、前記サービス要求に応じて、前記携帯端末に対し電子証明書を要求する電子証明書要求を送信する手順と、前記携帯端末から送信される電子証明書を受け、該電子証明書に基づき本人認証を行う手順と、前記本人認証で前記ユーザが正当なユーザであると判定された場合、前記サービス要求に応じたサービスを提供する手順と、を含むことを特徴とする。

【００１４】また、本発明の本人認証機能を有するサービス提供機器における処理方法において、該処理方法が、さらに、前記携帯端末から送信された電子証明書を、該電子証明書を発行し本人認証を行う認証機関の認証システムに転送する手順と、該認証システムから前記ユーザが正当なユーザであるか否かの判定結果からなる情報を受け、前記本人認証を行う手順と、を含むことを特徴とする。

【００１５】また、本発明は、コンピュータ装置にインストールすることにより、その装置が請求項８に記載の方法を実行する装置となるソフトウェアが記録されたコンピュータ読取可能な記録媒体である。

【００１６】また、本発明は、コンピュータ装置にインストールすることにより、その装置が請求項９または請求項１０に記載の方法を実行する装置となるソフトウェアが記録されたコンピュータ読取可能な記録媒体である。

【００１７】

【発明の実施の形態】以下、本発明の実施の形態を、図面を参照して説明する。図１は、本発明の一実施の形態である携帯端末およびサービス提供機器とさらに認証機関の認証システムからなるシステムの構成を示すブロック図である。なお、本実施の形態では、携帯端末とサービス提供機器間で無線通信を行うものとして説明するが、携帯端末とサービス提供機器間の通信は、無線通信に限定されるものではない。

【００１８】符号Ｔは、下記の使用者認証部１とサービスアクセス部２と証明書送信部３と証明書格納部４とをもつ携帯端末を示している。この携帯端末Ｔは、例えば、携帯電話端末や、無線通信可能なＰＤＡ（Ｐｅｒｓｏｎａｌ Ｄａｔａ Ａｓｓｉｓｔａｎｔｓ）や小型ノートＰＣ等を用いて実現される。

【００１９】証明書格納部４は、認証機関によって発行された電子証明書のデータ（以下、この電子証明書のデータを電子証明書と称す）と、携帯端末Ｔにおいて行う使用者認証用のデータ（個人識別情報）となるパスワード、指紋等の情報を格納している。証明書格納部４に格納される電子証明書は、所有者固有の情報をもち、例えば、個人を識別するＩＤ（識別番号等）と証明書用のデータとからなる。また、証明書格納部４は、具体的には携帯端末Ｔ内の内蔵メモリや、携帯端末Ｔに接続される着脱可能なメモリカード等の記憶媒体を用いて構成される。そしてまた、この証明書格納部４は、格納された情報の改竄を防止するため、任意の消去・更新ができないように構成されている。また上記のように、証明書格納部４を着脱可能なメモリカードを用いて構成した場合、他の携帯端末に装着して利用することもできる。

【００２０】使用者認証部１は、電子証明書を使用しようとしている人が、電子証明書を使用できる本人であるかどうか、パスワードの入力や使用者の指紋の入力等により使用者を認証する機能をもつ。この認証により使用者が正当であることが確認されると電子証明書の使用が許可される。

【００２１】サービスアクセス部２は、後述する各種サービス提供機器Ｓに組み込まれるサービス受付部５への接続要求と、サービス受付部５から携帯端末Ｔに送られる接続用アプリケーションプログラムの受信とその実行を行う機能をもつ。例えば、この接続用アプリケーションプログラムがＪａｖａアプレットとして構成される場合、サービスアクセス部２には、ＪａｖａＶＭ（Ｊａｖａ Ｖｉｒｔｕａｌ Ｍａｃｈｉｎｅ）が組み込まれ、このプログラムを実行する。この接続用アプリケーションプログラムにより、携帯端末Ｔの表示部（図示せず）には、サービス提供機器Ｓと通信し認証を行うためや、サービス提供機器Ｓを操作するためあるいはサービス提供機器Ｓが提供するサービスを享受するための、このサービス提供機器Ｓに固有の画面メニューが表示される。そして、この携帯端末Ｔは、サービス提供機器Ｓが提供する接続アプリケーションによっては、サービス提供機器Ｓに対応したリモコンのように使用することもできるようになり、使用者により指定されたサービスを要求するサービス要求をサービス提供機器Ｓに向け送信する。また、携帯端末Ｔは、ユーザの意図的な動作により最も近接した（例えば、最初に応答した）各種サービス提供機器と接続されるが、複数のサービス提供機器Ｓが同時に応答した場合、表示部にこれらのいずれかを選択するメニューを表示させ、ユーザに選択させるようにしてもよい。

【００２２】証明書送信部３は、サービス提供機器Ｓから送られる電子証明書要求の受信と、この電子証明書要

求に応じて電子証明書を送信する機能をもつ。なお、電子証明書を送信する際に、暗号化を行うことにより、さらにセキュリティを高めることができる。またこの暗号化は、電子証明書の送信を無線通信により行うことから、電子証明書の送信毎に、暗号化の方式や暗号化に用いる暗号鍵等を異なるようにすることが望ましい。

【００２３】次に、符号Ｓは、認証を伴うサービスを提供するサービス提供機器を示している。このサービス提供機器Ｓは、下記のサービス受付部５と、認証制御部６が組み込まれる。サービス受付部５は、携帯端末Ｔのサービスアクセス部２からの接続要求を受け付け、この接続要求に応じて、前述した接続用アプリケーションプログラムを送信する機能をもつ。この接続用アプリケーションプログラムを、携帯端末Ｔからの接続要求に応じて送るのは、様々なサービス提供機器Ｓを想定しているため、それぞれに固有の画面やメニューを携帯端末Ｔに表示させるためである。認証制御部６は、携帯端末Ｔに対する電子証明書の要求と、認証機関への電子証明書の転送、認証機関による認証結果の受信、サービス提供許可・不許可の判定の機能をもつ。なお、サービス提供機器Ｓと携帯端末Ｔ間は、近距離無線通信規格（Ｂｌｕｅｔｏｏｔｈ）等により無線で接続される。

【００２４】符号Ｃは、認証機関の認証システムを示している。この認証システムＣは、下記の認証実行部７と、個人情報蓄積部８とから構成される。認証実行部７は、各種サービス提供機器Ｓに組み込まれたサービス受付部５から転送された電子証明書の受信とその復号化をし、電子証明書に含まれる個人情報と下記の個人情報蓄積部に保存されている個人情報との照合をする。そして、その照合結果をサービス提供機器Ｓの認証制御部６へ送信する機能をもつ。個人情報格納部８は、電子証明書を発行した個人の情報（個人情報）を蓄積し管理する機能をもつ。この個人情報格納部８に格納される個人情報は、個人を識別するＩＤ（識別番号等）、電子証明書照合用データ、氏名、性別、年齢、住所、電話番号、その他所有者に属する情報からなっている。なお、個人情報格納部８は、ハードディスク、光磁気ディスク等の不揮発性の記録装置や記憶装置により構成され、あるいはまた、ネットワークを介して接続され個人情報を蓄積するサーバ・コンピュータ等により構成してもよい。

【００２５】また、上記携帯端末Ｔの使用者認証部１とサービスアクセス部２と証明書送信部３、サービス提供機器Ｓのサービス受付部５と認証制御部６、そして認証システムＣの認証実行部７の各機能は、メモリおよびＣＰＵ（中央演算装置）等により構成される処理部により、これらの各機能を実現するためのプログラム（図示せず）をメモリにロードして実行することによりその機能が実現されるものとする。

【００２６】次に、このように構成された本人認証機能を有する携帯端末Ｔおよびサービス提供機器Ｓとさらに認証機関の認証システムＣからなるシステムの利用時における動作について、図２を参照して説明する。

【００２７】はじめに、ユーザは、パスワード、指紋情報等の本人を特定することができる個人識別情報を、携帯端末Ｔに入力する。上記個人識別情報が入力されると使用者認証部１は、入力された情報が、正当なユーザを特定するものであるか否か判断する（ステップＳ１）。そして、この判断で、正当なユーザを特定するものであると判定された場合（ステップＳ１の判断でＹＥＳの判定）、電子証明書を使用可能な状態とする。ステップＳ１の判断でＮＯの判定された場合、電子証明書の使用を不許可にする（ステップＳ３）。

【００２８】次に、携帯端末Ｔのサービスアクセス部２は、ユーザからの操作に応じて、サービス提供機器Ｓのサービス受付部５に接続要求を無線通信により送信する（ステップＳ４）。

【００２９】次に、サービス受付部５は、携帯端末Ｔから接続要求を受けると（ステップＳ５）、接続用アプリケーションプログラムを携帯端末Ｔのサービスアクセス部２に送信する（ステップＳ６）。

【００３０】そして、サービスアクセス部２は、接続用アプリケーションプログラムを受信するとこのプログラムを実行する（ステップＳ７）。この接続用アプリケーションプログラムにより、携帯端末Ｔは、サービス提供機器Ｓから所望のサービスを受けるためのサービス要求を、サービス受付部５へ送ることができる。

【００３１】接続用アプリケーションプログラムを実行したサービスアクセス部２は、さらにユーザからの操作を受け、この操作に応じて、サービス受付部５にサービス要求を出す（ステップＳ８）。

【００３２】次に、サービス受付部５がサービスアクセス部２から送信されたサービス要求を受信すると（ステップＳ９）、認証制御部６が携帯端末Ｔの電子証明書を要求する証明書要求を送信する（ステップＳ１０）。

【００３３】証明書送信部３は、この証明書要求を受信すると（ステップＳ１１）、証明書格納部４から電子証明書を取得し、安全のため一度ユーザの確認を取った上で、この電子証明書を認証制御部６に送信する（ステップＳ１３）。この電子証明書の送信にあたり、前述したように、暗号化を行うことが望ましい。以下では、この電子証明書が暗号化され送信されるものとする（ステップＳ１２）。

【００３４】次に、認証制御部６は、暗号化された電子証明書を受信すると（ステップＳ１４）、認証機関の認証システムＣに備わる認証実行部７に電子証明書をそのまま転送する（ステップＳ１５）。

【００３５】認証実行部７は、暗号化された電子証明書を受信すると（ステップＳ１６）、受信した電子証明書を復号化し（ステップＳ１７）、その情報と個人情報格納部８に格納されたユーザの個人情報とを照合した上

（ステップＳ１８）、その結果（照合結果）を認証制御部６に返す（ステップＳ１９）。ここで返信される照合結果には、本人性の肯定／否定の判定結果と個人情報の一部（例えば、住所等）を含む。

【００３６】認証制御部６は、上記照合結果を受けると（ステップＳ２０）、この照合結果を判定し（ステップＳ２１）、本人性が保証された場合（ステップＳ２１の判断でＯＫと判定された場合）はサービス開始を許可し（ステップＳ２２）、本人性が保証されなかった場合（ステップＳ２１の判断でＮＯと判定された場合）は、その本人性を否定する通知（ＮＧ）を証明書送信部３に送信する（ステップＳ２３）。

【００３７】証明書送信部３が、本人性を否定する通知を受信すると、証明書送信部３は、サービス提供機器Ｓにおける本人認証において、本人性が確認されなかったことをユーザに伝えるメッセージを表示させる（ステップＳ２４）。

【００３８】以上、本人認証機能を有する携帯端末Ｔおよびサービス提供機器Ｓとさらに認証機関の認証システムＣからなるシステムの利用時における動作について説明した。なお、上記で説明した動作フローは一例であり、上記の処理の流れに限定されるものではない。本実施の形態では、携帯端末Ｔを使って本人認証（個人の認証）を行っているが、使用者認証部１とサービスアクセス部２と証明書送信部３と証明書格納部４を物・装置（例えば、自動車等）に組み込んで、その物の認証を行うようにしてもよい。

【００３９】次に、サービス提供機器Ｓが、自動車に搭載される車載器として実施された場合の実施例を、図３、４を参照して説明する。

【００４０】本実施例では、事前に車載器に搭乗を許可するユーザを登録しておく。ユーザは、電子証明書を記憶した携帯端末Ｔを用いて、無線通信により車載器に接続し、要求に応じて電子証明書を送信する。携帯端末Ｔから電子証明書を受けた車載器は、認証機関にこの電子証明書を転送する。そして、電子証明書を受けた認証機関の認証システムＣは、当該ユーザが本人であるか否かを認証する。そしてさらに認証機関の認証システムＣは、当該ユーザが運転免許を取得しているかどうかを警察システムに問い合わせる。認証機関において、本人認証とユーザの自動車免許に係る認証が正常に完了した場合、その認証結果を車載器に送信する。車載器は、この認証結果を受信すると、ドアを開錠し、エンジンスタートを許可する。

【００４１】また、本人認証を完了した車載器は、事前にこのユーザ用に設定してあるシートやミラーの位置、オーディオの設定などの調節を、これらを制御する車内システムにリクエストする。さらに、車載器は、認証済みユーザの個人専用ポータルサイトにネットワークを介してログインし、この個人専用ポータルサイトに事前に設定してある一般ポータルや契約ＡＳＰ（アプリケーション・サービス・プロバイダ：保険会社、決済機関、情報提供会社…）等を組み合わせて、当該ユーザに最適な利用環境を構築する。本システムにより、サービス提供側は、常に本人である確証を得た状態でサービスを提供することができる。また、車載器は警察からのアクセスがあった場合は、常に電子証明書を提示できるよう待機している。警察は違反車両を発見した場合、その車両にアクセスして電子証明書を提示させ、免許関連のデータベースに違反情報を登録する作業や、違反者に通知する作業をすべて遠隔で自動的に済ますことが可能となる。

【００４２】次に、他の実施例を、図５～８を参照して説明する。本実施例は、自動車にトラブルが発生した場合にサービスを提供する例である。

【００４３】図５，６は、本実施例の構成を示している。本実施例では、図５に示す無線通信可能な自動車と、この自動車と無線で接続される無線局と、この無線局からインターネット等の通信インフラを介して接続されるヘルプセンター（自動車の緊急時にサービスを提供するセンター）と自動車ディーラから構成される。また、これらには、Ｊａｖａで記述されたエージェントプログラム（Ａｇｅｎｔ）とこのプログラムを実行するプロセッサが組み込まれており、情報の授受を行う。また、図６に示すように、ヘルプセンター（ＨＥＬＰセンター事業者）と自動車ディーラ（自動車ディーラＡＳＰ事業者）のサーバへは、ポータルサイトのサーバ（Ｐｏｒｔａｌ　Ｓｅｒｖｅｒ）を介してもよい。

【００４４】次に、本実施例において、ヘルプセンターが自動車の異常を検知しサービスを提供する前に行う認証処理の過程を説明する（図７参照）。

【００４５】自動車には、Ｊａｖａで記述されたエージェントプログラムとこのプログラムを実行するプロセッサが組み込まれており、ヘルプセンターは、このエージェントプログラムにより、自動車内の各部の制御情報を、無線通信およびインターネット等の通信インフラを介して、モニタ可能な状態にある。誰かがこの自動車に搭乗しようとすると、エージェントプログラムにより、搭乗しようとする人物が使用する携帯端末Ｔから受けたこの人物の電子証明書とこの自動車の車体ＩＤがヘルプセンターへ送られる。この電子証明書に基づく個人情報と車体ＩＤをもとに、自動車ディーラから、搭乗しようとしている人物が正規の登録会員であるか否かの情報を得る。このとき、正規の登録会員ではない人物が搭乗しようとした場合、ヘルプセンターは異常として検知する。そして、この自動車に対し使用を不許可にする制御を行うとともに、正規の登録会員に携帯電話等を用いて確認の通知を行う。

【００４６】次は、本実施例で、自動車に発生した緊急のトラブルに対し支援するサービスを提供する場合の例である（図８参照）。

【００４７】自動車に破損等の事故が発生した場合、この自動車に組み込まれたエージェントプログラムにより、車体ＩＤを含む破損情報とドライバの電子証明書がヘルプセンターへ送られる。ヘルプセンターは、ドライバの電子証明書と車体ＩＤから自動車ディーラのサーバへアクセスし、車両情報等を得る。そして、異常状態により、通知の必要な各種事業者・機関（警察・病院・ロードサービスなど）を自動的に決定し、必要な情報を送る。このように、破損情報を受信したヘルプセンターは、異常状況の詳細を知ることができ、必要なサービスを直ちに実行できる。以上、本実施の形態の実施例を説明した。

【００４８】本実施の形態の基となる特許請求の範囲に記載した発明は、現実世界で本人認証のために用いられている各種証明書を電子化し、個人で使用できる携帯端末に記憶させて使用するという発想のもとになされた。この発明は、近距離無線通信、組み込みＯＳ・Ｊａｖａ等の技術を用いることにより、あらゆる機器に認証のためのインターフェースを設け実施することが可能であり、携帯電話端末などの携帯端末も接続用アプリケーションプログラムの実行やサービス提供機器側との会話的な通信が可能となる。よって、ユーザは上記発明による携帯端末さえ持ち歩けば、本人認証を必要とする様々なサービス提供機器を相手に、簡単な操作のみで確実な本人認証を行うことができる。

【００４９】また、他の実施の形態として、前述した実施の形態の携帯端末Ｔの構成要素を各種サービス提供装置Ｓに備え、さらに、前述した実施の形態の各種サービス提供装置Ｓの構成要素を携帯端末Ｔに備えることにより、携帯端末Ｔ側においても、各種サービス提供装置Ｓに対する認証を行うようにしてもよい。本構成をとることにより、各種サービス提供装置から提供されるサービスが、正しくそのサービスの提供者によるものか確認することができる。

【００５０】なお、図１における携帯端末Ｔの使用者認証部１とサービスアクセス部２と証明書送信部３の機能を実現するためのプログラムと、サービス提供機器Ｓのサービス受付部５と認証制御部６の機能を実現するためのプログラムを、それぞれコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムを、それぞれ携帯端末Ｔに対応するコンピュータシステムとサービス提供機器Ｓに対応するコンピュータシステムに読み込ませ、実行することにより本人認証機能を有する携帯端末ＴおよびサービスＳからなるシステムを構成してもよい。なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものとする。

【００５１】また、「コンピュータシステム」は、ＷＷＷシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フロッピー（登録商標）ディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（ＲＡＭ）のように、一定時間プログラムを保持しているものも含むものとする。

【００５２】また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

【００５３】以上、この発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【００５４】

【発明の効果】以上、詳細に説明したように、本発明によれば、個人的に使用される携帯端末に本人性を保証する電子証明書を記憶させることにより、場所に縛られることなく、認証を伴うサービスの提供と享受を実現することができる。また、ユーザは自分の携帯端末を用いて、サービスを提供するサービス提供機器と無線通信による接続を要求するだけで、様々なサービス提供機器と接続し、そのサービスを受けることができる。また、ユーザは、サービス提供機器から送られる接続用アプリケーションプログラムにより、簡単な操作をするだけで、サービス提供機器と携帯端末間で認証を完了し、サービス提供機器固有のサービスを享受できる。また、サービス提供者は、本発明のシステムにより、ユーザの居場所にとらわれることなく、本人認証を伴う様々な自動サービスを展開することができる。また、認証機関は、認証を伴うサービスの普及が進み、利用者の増加につながる。また、本発明では、携帯端末上で使用者の本人認証を行い、さらにサービス提供機器において認証機関による本人認証を行う二重の認証により、本人認証を確実なものとしている。

【図面の簡単な説明】

【図１】　本発明の一実施の形態である携帯端末および

サービス提供機器と認証機関の認証システムからなるシステムの構成を示すブロック図である。

【図２】　同実施の形態の動作を説明する図である。

【図３】　同実施の形態の一実施例を示す図である。

【図４】　同実施の形態の一実施例を示す図である。

【図５】　同実施の形態の一実施例の構成を示す図である。

【図６】　同実施の形態の一実施例の構成を示す図である。

【図７】　同実施の形態の一実施例の動作を説明する図である。

【図８】　同実施の形態の一実施例の動作を説明する図である。

【符号の説明】

１…使用者認証部　　２…サービスアクセス部

３…証明書送信部　　４…証明書格納部

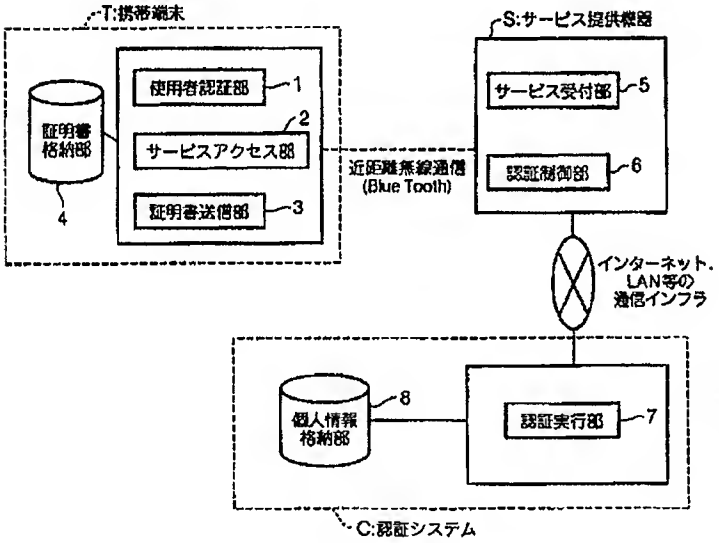
５…サービス受付部　　６…認証制御部

７…認証実行部　　８…個人情報格納部

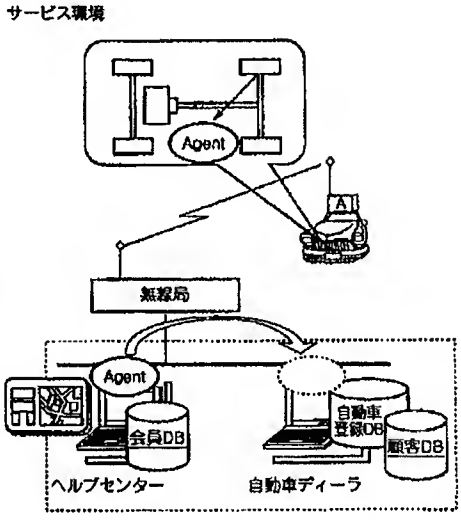
Ｔ…携帯端末　　Ｓ…サービス提供機器

Ｃ…認証システム

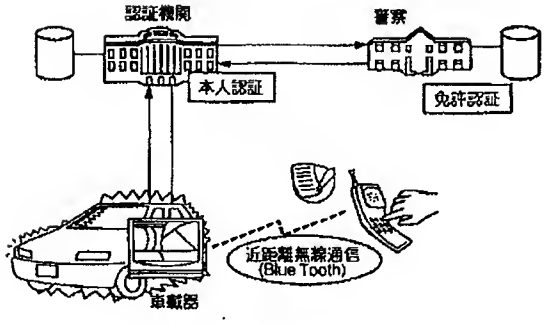
【図１】



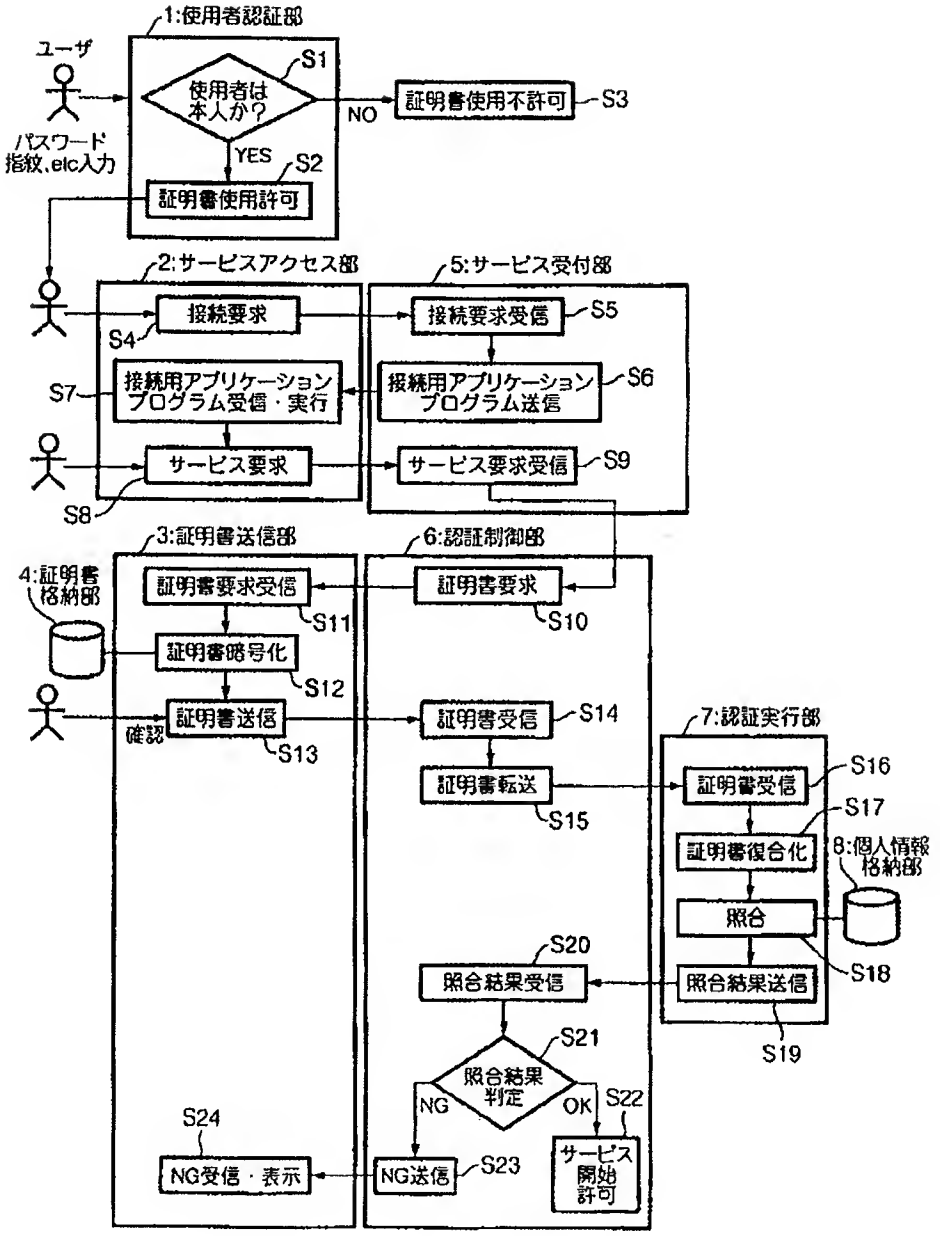
【図５】



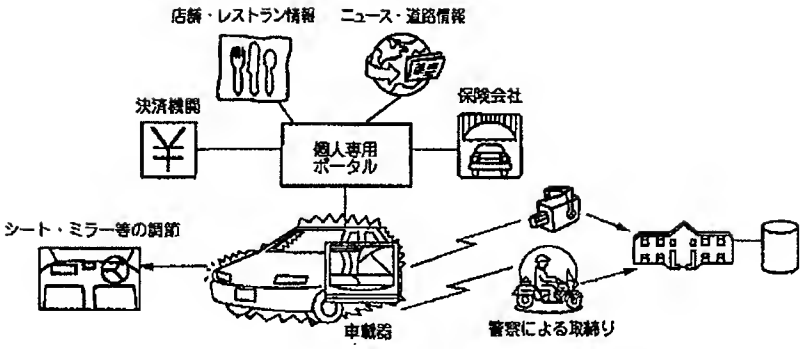
【図３】



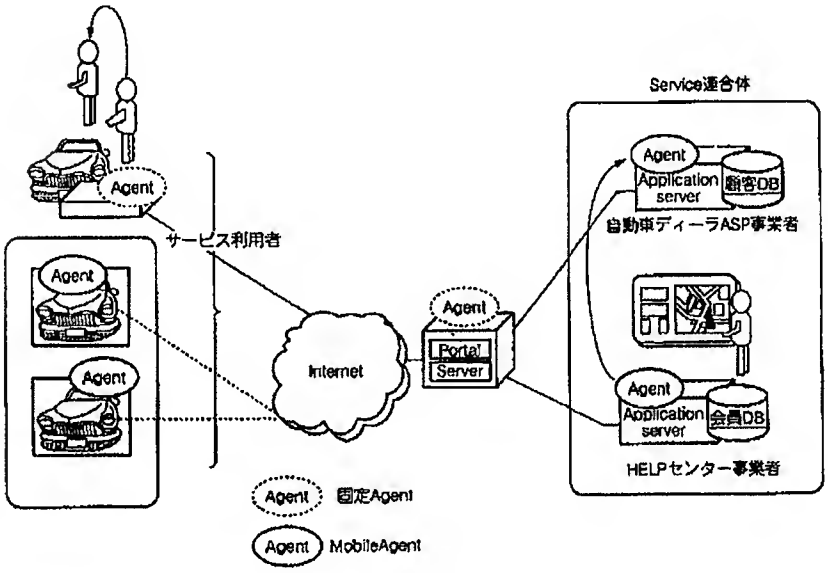
【図２】


1:使用者認証部
ユーザ
使用者は本人か？
S1
NO
証明書使用不許可
S3
パスワード
指紋、etc入力
YES
S2
証明書使用許可
2:サービスアクセス部
5:サービス受付部
接続要求
S4
接続要求受信
S5
接続用アプリケーションプログラム受信・実行
S7
接続用アプリケーションプログラム送信
S6
サービス要求
S8
サービス要求受信
S9
3:証明書送信部
6:認証制御部
4:証明書格納部
証明書要求受信
S11
証明書要求
S10
証明書暗号化
S12
確認
証明書送信
S13
証明書受信
S14
7:認証実行部
証明書転送
S15
証明書受信
S16
S17
証明書復合化
8:個人情報格納部
照合
S18
S20
照合結果受信
照合結果送信
S19
S21
照合結果判定
NG
OK
S22
S24
NG受信・表示
NG送信
S23
サービス開始許可

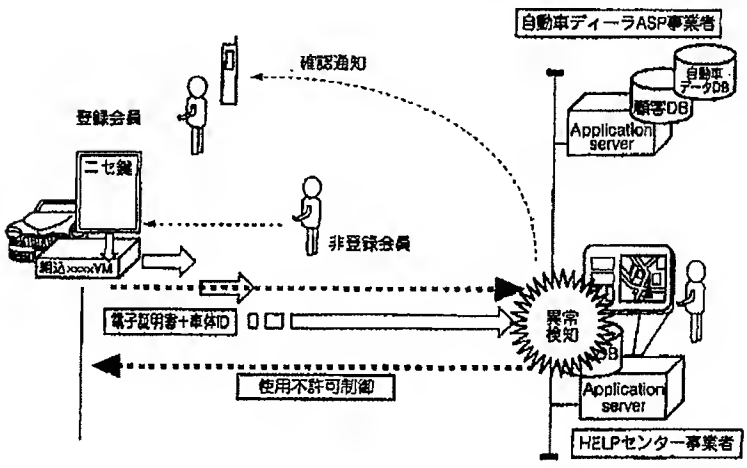
【図４】


店舗・レストラン情報
ニュース・道路情報
決済機関
保険会社
個人専用
ポータル
シート・ミラー等の調節
車載器
警察による取締り

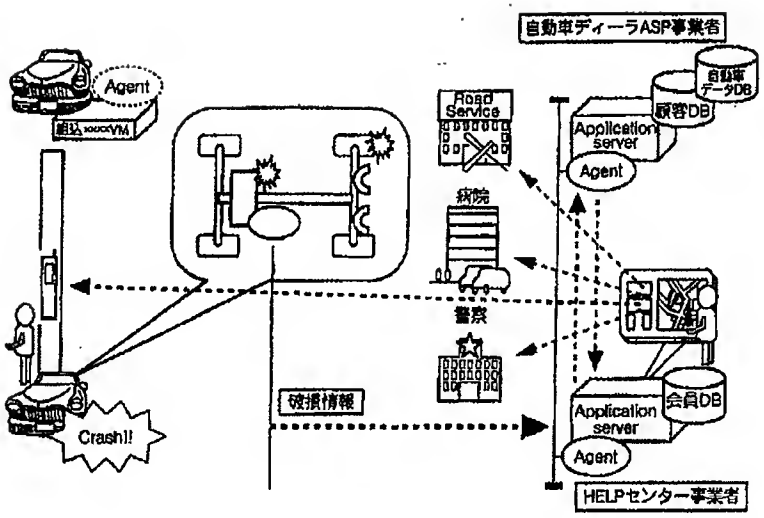
【図６】


Service連合体
Agent
Application server
顧客DB
自動車ディーラASP事業者
サービス利用者
Agent
Internet
Agent
Portal Server
Agent
Application server
会員DB
HELPセンター事業者
Agent
固定Agent
Agent
MobileAgent

【図７】


自動車ディーラASP事業者
確認通知
登録会員
自動車データDB
顧客DB
Application server
ニセ鍵
非登録会員
電子取扱書+車体ID
異常検知
使用不許可制御
Application server
HELPセンター事業者

【図８】



フロントページの続き

(72)発明者　大室　久子
東京都港区港南一丁目９番１号　エヌ・ティ・ティ・コミュニケーションウェア株式会社内
(72)発明者　長岡　亨
東京都港区港南一丁目９番１号　エヌ・ティ・ティ・コミュニケーションウェア株式会社内
(72)発明者　小林　和恵
東京都港区港南一丁目９番１号　エヌ・ティ・ティ・コミュニケーションウェア株式会社内

Ｆターム(参考)　5B085 AE23
5J104 AA07 KA01 KA06 KA17 MA01 NA05 NA35 NA36 NA41 NA42
5K067 AA32 AA33 BB04 DD17 EE02 EE10 EE22 EE35 FF07 FF23 HH17 HH22 HH23 HH24 HH36 KK15